
Quantum Network Protocols: for Quantum Key Distribution (QKD)

Deborah Jackson
David Gilliam
Jonathan Dowling

Jet Propulsion Laboratory
California Institute of Technology
Pasadena, CA

Requirements for Quantum Communications



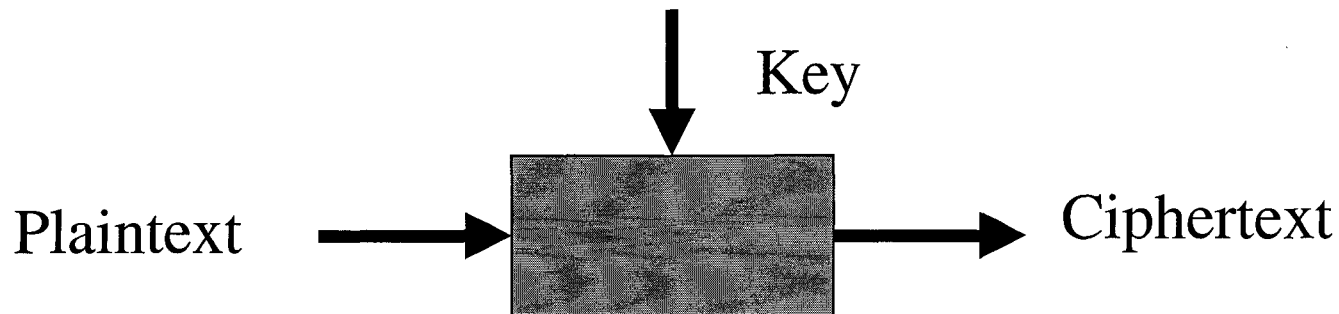
-
- Qubits definition- any 2-state quantum system
 - Particle spin
 - Photon polarization
 - Discrete atomic or molecular energy levels
 - Current flow direction in Josephson junction loops
 - DiVincenzo's determinations [2000]
 - Ability to interconvert stationary and flying qubits.
 - Ability to faithfully transmit flying qubits between specified locations.
 - Communications applications
 - Secret key distribution (QKD)
 - Multi party functions
 - Collaborative workflow (networking)
 - Distributed quantum computing
 - Clock synchronization

Ref: arXiv:quant-ph/0002077 (April 2000)

Drivers for QKD Implementation



-
- Key exchange weakest part of crypto procedure
 - Symmetric => Asymmetric
 - Impact of computational trends
 - Networking through the internet provides easy access to computational power for deciphering encryption algorithms.
 - Onset of quantum computers and other parallel processing methods attack confidence in most algorithmic encryption methods.
 - Solution: QKD + Vernam Cipher = One Time Pad

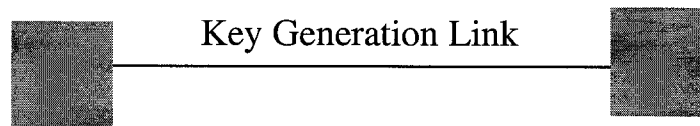


2-node QKD Key Generation Sequence

JPL

Alice

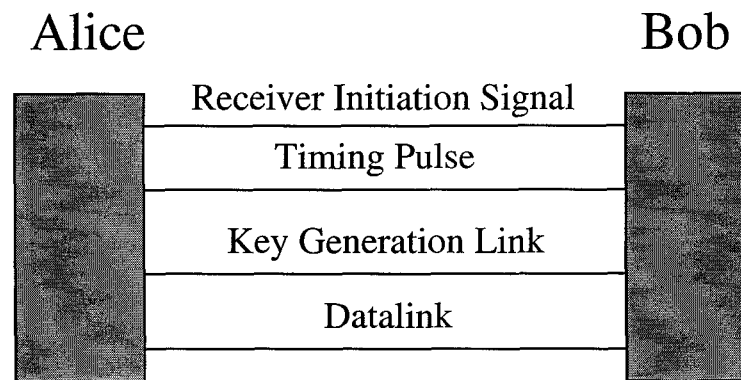
Bob



- QKD demonstrated over 49 km of dedicated experimental fiber by LANL.
- British Telecom demonstrated over 30 km of datalink; no degradation of QKD signal.

2-node QKD Key Generation Sequence

JPL

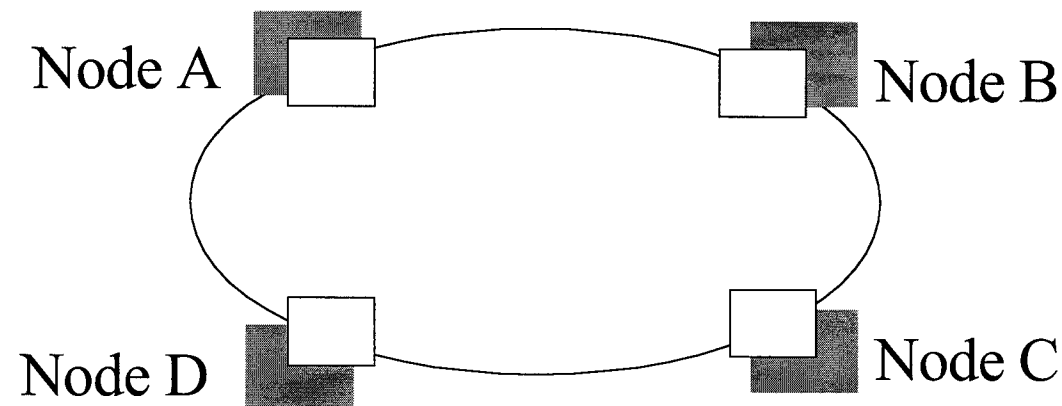


- Initiation broadcast from Bob indicates reception availability.
- Timing pulse from Alice provides reference for gated detection of photon.
- Alice generates photons through a random polarization; Bob detects photons with random polarization.
- Alice and Bob compare notes via communications on a data link to mutually establish random keys.



Qubit distribution in multiple node LAN

JPL

Quantum Internet Testbed Network



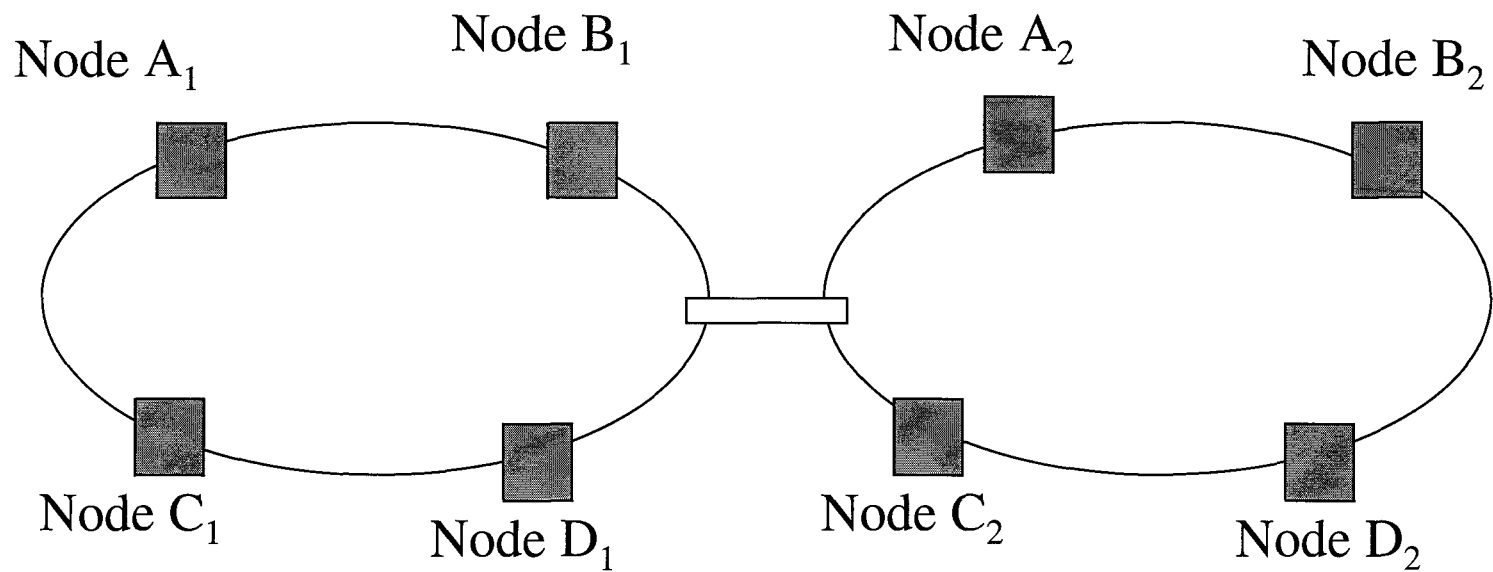
Legend:

-  Delay loop interface for timing control
-  Quantum computer or experiment at the node

Additional control functions needed:

- Authentication protocol
- Dis-associated routing header

Scaling up to Larger N

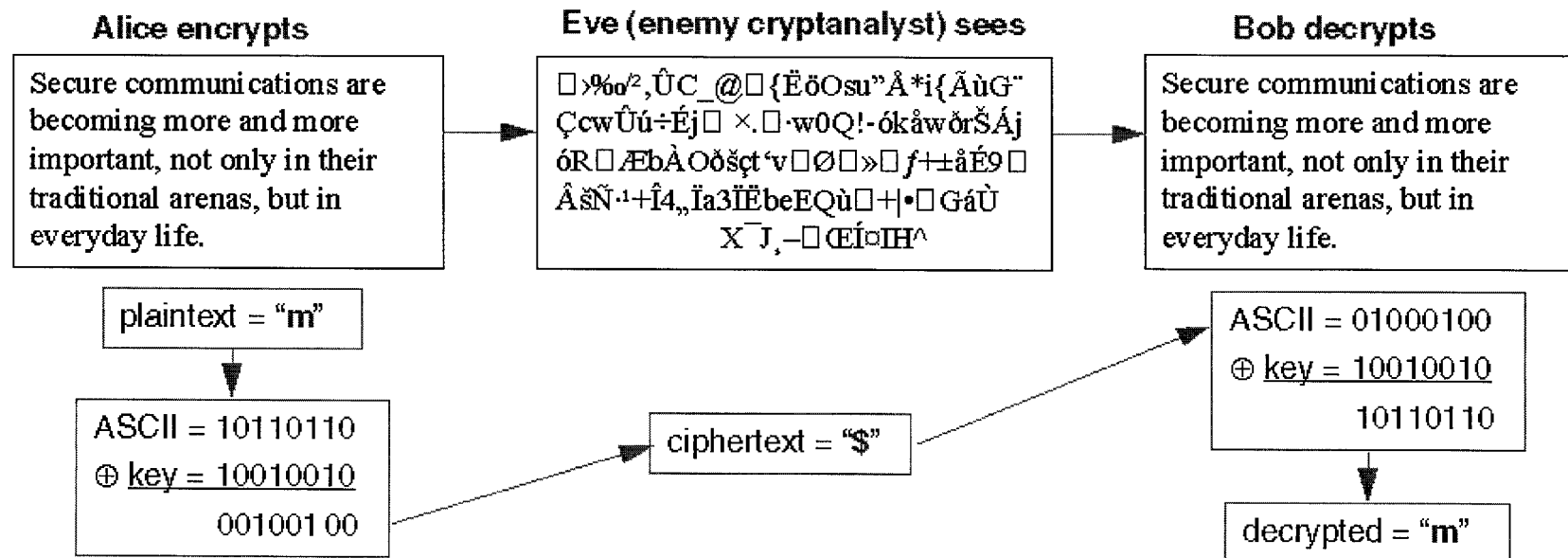


Example of (Quantum) Cryptography

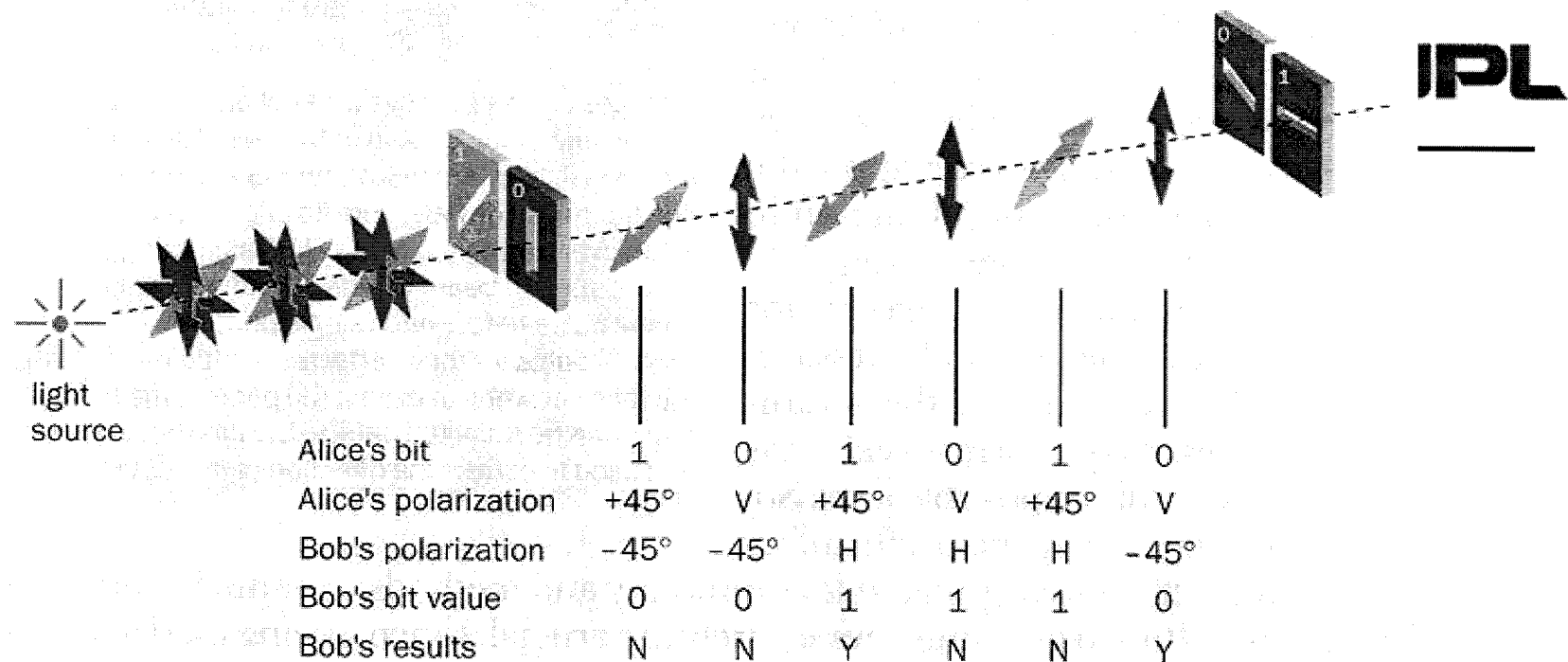
- Alice and Bob generate shared key material (random numbers) using **single photon transmissions** of quantum cryptography over 14 km of optical fiber
- e.g. use of key for “one-time pad” **encryption/decryption** of short messages:

Sample of key material

B	00001010	01111111	01010111	01011010	00010011
A	00001010	01111111	01010111	01011010	00010001
B	00000011	11100111	11011111	00000100	00001100
A	00000011	11100111	11011111	00000100	00001100
B	10110100	11101110	01110000	10100101	11111001
A	10110100	11101110	01110000	10100101	11111001
B	00110100	01001000	10000000	10111111	01010101
A	00110100	01001000	10000000	10111111	01010101
B	10111111	00000000	00100010	01011000	11011010
A	10111011	01000000	00100010	01011000	11011010



1 Cryptography with polarized light



Quantum cryptography is a way of generating a shared key to encrypt and decrypt a message with absolute secrecy from a sequence of bits (row 1). In the B92 protocol, Alice has two filters that can linearly polarize photons vertically (V) or at +45°. For each photon she sends through free space, she chooses one of these filters at random (row 2). Bob has analysers that can measure photons that are polarized in the horizontal (H) or -45°. Every time he expects a photon to arrive, he selects one of the polarizers at random (row 3) that correspond to bit values (row 4). He records whether or not he detects a signal and communicates this information to Alice over a public channel (row 5). Alice and Bob only retain the bits for which Bob detected a photon and they use these as a secret key. Bob will never detect the photon if he selects an analyser that is incompatible with Alice's polarizer (columns 1 and 4). In the case where he does chose a compatible analyser, he has a 50% chance of detecting the photon (columns 2, 3, 5 and 6).

Basic Requirements for Quantum Computing Implementation



DiVincenzo's determinations [2000]

1. Scalable physical system; i.e. 2^n dimensional complex vector from n-qubits
 2. Ability to initialize qubits in simple fiducial state; e.g. $|000\dots\rangle$
 3. Decoherence time $>$ gate operation time
 4. Universal set of quantum gates
 5. Qubit specific measurement capability
- Need to add some form of timing control.

Ref: arXiv:quant-ph/0002077 (April 2000)

JPL

